Security Advisory Ransomware

Ransomware (auch Erpressungstrojaner, Kryptotrojaner oder Verschlüsselungstrojaner genannt) bezeichnet Schadprogramme, die den Zugriff auf Daten oder auf das ganze Computersystem verhindern können. Bei einem erfolgreichen Angriff werden Daten auf dem Computer durch kryptologische Verfahren verschlüsselt. Die Wiederherstellung der verschlüsselten Daten ist nur mit dem passenden Schlüssel möglich, für dessen Bereitstellung ein Lösegeld gefordert wird.

Ransomware verbreitet sich über Sicherheitslücken in Microsoft Windows Betriebssystemen. Die häufigsten Angriffe erfolgen über Spam-E-Mails mit ausführbaren Dateien (z. B. doc, xls, docx, zip, rar, exe), die von unvorsichtigen Anwendern geöffnet werden. Eine Angriff kann aber auch durch eine mit Malware versehene Web-Seite erfolgen, die eine Sicherheitslücke im verwendeten Web-Browser ausnutzt (Drive-by-Exploit).

Aktuell nutzen Cyber-Kriminelle insbesondere Varianten aus den Ransomware-Familien ***WannaCry*** und ***Petya*** für digitale Erpressungsversuche.

Gefährdung

Grundsätzlich gefährdet sind alle **Computersysteme mit Microsoft Windows Betriebssystemen** und damit auch verschiedene Dallmeier Produkte wie beispielsweise:

- Workstation Tower (004904)
- Workstation Rack-Mount 4RU (004903)
- Server Rack-Mount 1RU (004847)
- Abgekündigte Produkte wie PView Station 7 (000307) oder SeMSy® III Workstation Hardware (003304)

Dallmeier Produkte mit Windows Betriebssystem werden immer mit den zum Zeitpunkt der Produktion aktuellen Updates und Sicherheits-Patches ausgeliefert.

*Dallmeier **Aufzeichnungssysteme** sind mit einem in Hinblick auf die Systemsicherheit stark angepassten und abgeschotteten (hardened) **Linux Betriebssystem** ausgestattet. Sie sind auch durch die aktuell kursierende Ransomware **nicht gefährdet**.*

Maßnahmen

Grundsätzlich sollte das **Microsoft Windows Betriebssystem** immer auf dem **aktuellen Stand** gehalten werden. Dies kann direkt über die Update-Funktion des Betriebssystems erfolgen. Microsoft informiert aber auch auf der folgenden Web-Seite über die Verfügbarkeit von Sicherheits-Patches für die verschiedenen Betriebssysteme und Plattformen (32 oder 64 Bit):

Allgemein https://technet.microsoft.com/en-us/library/security/dn631937.aspx
WannaCry https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Zudem bietet Microsoft den direkten Download von Updates an, die über einen USB-Stick auf dem entsprechenden Computersystem installiert werden können. Beispielsweise ein Patch für die aktuell ausgenutzte SMB-Sicherheitslücke für Microsoft Windows 7 64 Bit oder Microsoft Windows 10 Build 1607.

Halten Sie Computersysteme mit Windows Betriebssystem durch aktuelle Updates und Sicherheits-Patches immer auf dem aktuellen Stand.

Neben einem aktuellen Betriebssystem sollten **grundsätzlich** die etablierten **Maßnahmen und Vorgehensweisen der IT-Sicherheit** beachtet werden. Ausführliche Informationen zu diesem Thema bietet beispielsweise das **Lagedossier Ransomware** des Bundesamt für Sicherheit in der Informationstechnik.

- Durchführung regelmäßiger Backups von wichtigen Daten
- Einsatz aktueller Virenschutzprogramme
- Einsatz aktueller Web-Browser
- Vermeidung der Ausführung verdächtiger Dateien
- Vermeidung der Ausführung von Skripten oder Makros
- Mitarbeitersensibilisierung

Starten Sie niemals eine ausführbare Dateie, die Ihnen nicht hundertprozentig vertrauenswürdig erscheint. Sensibilisieren Sie diesbezüglich Ihre Mitarbeiter.

Windows XP

Computersysteme mit einem **Microsoft Windows XP** Betriebssystem sollten unverzüglich **vom Netzwerk und insbesondere vom Internet abgetrennt** werden.

Das **Windows XP** Betriebssystem ist hoffnungslos **veraltet** (End of Life). Microsoft bietet seit 2014 **keine Updates und keinen Support** mehr an (End of Support). Weitere Informationen gibt Microsoft auf folgender Web-Seite:

https://www.microsoft.com/en-us/windowsforbusiness/end-of-xp-support

Für die von ***WannaCry*** ausgenutzte Sicherheitslücke hat Microsoft trotz des Support-Endes ein **Sicherheits-Patch** zur Verfügung gestellt. Dieses kann über das Internet direkt von Microsoft bezogen und über einen USB-Stick auf dem vom Netzwerk getrennten Windows XP System installiert werden. **Von einem weiteren Einsatz des Windows XP Systems wird dennoch dringend abgeraten**, da dieses Sicherheits-Patch **nur eine von vielen bekannten Sicherheitslücken** behebt.

Das Dallmeier Sales-Team oder Ihr Vertriebspartner beraten Sie gerne bezüglich einer Migration auf Computersysteme mit modernem Microsoft Windows 10 Betriebssystem.